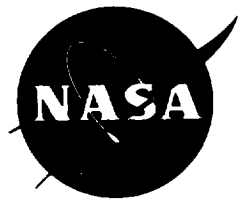
(67)

OFFICE OF MANNED SPACE FLIGHT

SAFETY PROGRAM DIRECTIVE NO. 1

SYSTEM SAFETY REQUIREMENTS FOR MANNED SPACE FLIGHT

JANUARY 1969



PREPARED BY MANNED SPACE FLIGHT SAFETY OFFICE
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, D. C. 20546

SYSTEM SAFETY REQUIREMENTS FOR MANNED SPACE FLIGHT

This Manned Space Flight Safety Program Directive establishes the system safety requirements for Manned Space Flight Programs.

All Manned Space Flight Programs or activities initiated after the date of this issuance shall select from these requirements applicable tasks and place them in individual procurement contracts and statements of work.

This Directive has been prepared under the authority of NASA Management Instruction 1138.12, Functions and Authority, Director, Manned Space Flight Safety; NASA Management Instruction 1700.2, Manned Space Flight Safety Program; and in accordance with NHB 1700.1, NASA Safety Manual.

Director, Manned Space Flight Safety Office

SYSTEM SAFETY REQUIREMENTS FOR
MANNED SPACE FLIGHT

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

SYSTEM SAFETY REQUIREMENTS FOR MANNED SPACE FLIGHT

SECTION 1

SCOPE

1.1 PURPOSE

The purpose of this document is to establish system safety requirements for Manned Space Flight Program Offices, Centers and installations participating in NASA Manned Space Flight Programs.

1.2 APPLICATION

Center Program Safety Offices will select from this document the applicable tasks and place them in individual procurement contracts and statements-of-work. The Center Program Offices should compare the benefits to be derived with the problems of implementation and coordinate any major deviations with the appropriate Safety Director, Headquarters Program Office.

In the application of these requirements, care shall be exercised to avoid conflicts between technical disciplines, to establish an integrated effort and to avoid duplication of effort by capitalizing on the use of existing data.

SYSTEM SAFETY REQUIREMENTS FOR MANNED SPACE FLIGHT

SECTION 2

DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents form a part of this issuance to the extent specified herein.

NPD 1701.1	Basic Policy on Safety
NMI 1138.12	Functions and Authorities—Director, Manned Space Flight Safety Office
NMI 1136.8A	Functions and Authorities—NASA Safety Director
NMI 1700.2	Manned Space Flight Safety Program

2.2 REFERENCES

NHB 1700.1	NASA Safety Manual
NHB 7121.1	Phase Project Planning Guidelines
AFSC DH 1-6	System Safety Design Handbook
AFETRM 127-1	Range Safety Manual
	Accident/Incident/Mission Failure Reporting and Investigating Handbook Interim Draft, 5 November 1968

SYSTEM SAFETY REQUIREMENTS FOR
MANNED SPACE FLIGHT

SECTION 3

DEFINITIONS

3.1 SAFETY TERMS

The following terms used in this document are defined:

a. Safety—Freedom from chance of injury or loss to personnel, equipment or property.
b. System Safety—The optimum degree of risk management within the constraints of operational effectiveness, time and cost attained through the application of management and engineering principles throughout all phases of a program.
c. Accident Prevention—Methods and procedures used to eliminate the causes which lead, or could lead, to an accident.
d. Hazard—The presence of a potential risk situation caused by an unsafe act or condition.
e. Risk—The chance of injury or loss to personnel, equipment or property.
f. Major Damage—Damage to equipment which results in major system degradation or loss.
g. Major System Degradation—A condition which results in one or more of the following:
   (1) Jeopardized achievement of an operation or performance of a mission; or delay beyond acceptable time limits.
   (2) Inadvertent system activation.

3.2 HAZARD CATEGORIES

Identified system hazardous conditions shall be categorized as follows:

a. Safety Catastrophic—Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem or component malfunction will severely degrade system performance, and cause subsequent system loss, death, or multiple injuries to personnel.
b. Safety Critical—Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or

subsystem or component malfunction will cause equipment damage or personnel injury, or will result in a hazard requiring immediate corrective action for personnel or system survival.

c. Safety Marginal—Condition(s) such that environment, personnel error, design characteristics, procedural deficiencies, or subsystem failure or component malfunction will degrade system performance but which can be counteracted or controlled without major damage or any injury to personnel.

d. Safety Negligible—Condition(s) such that personnel error, design characteristics, procedural deficiencies, or subsystem failure or component malfunction will not result in major system degradation, and will not produce system functional damage or personnel injury.

SYSTEM SAFETY REQUIREMENTS FOR
MANNED SPACE FLIGHT

SECTION 4

REQUIREMENTS

4.1 SYSTEM SAFETY PLAN (SSP)

An SSP prepared in accordance with the requirements of this document shall be prepared by the Contractor or by NASA for in-house work. The SSP, as approved by the procuring activity and incorporated into the contract, becomes the basis for contractual compliance. The plan must describe an integrated effort within the total project; it shall indicate how other systems analyses (i.e., failure modes and effects analyses) will be used to preclude duplication of analytical work. Existing documents may be referenced and submitted as part of the System Safety Plan.

The System Safety Plan shall contain a description of the system safety elements, as described below, which are considered necessary to insure effective management of a system safety program compatible with the NASA Safety Manual, NHB 1700.1.

4.1.1 Organization

The plan shall: (1) identify the organization and key personnel responsible for managing the overall system safety program, and (2) clearly define the responsibilities and functions of those directly associated with system safety policies and implementation. It shall stipulate the authority delegated to this organization to implement its policies. The relationship between line, staff, and interdepartmental, project functional, and general management organizations shall be identified.

4.1.2 Management and Control

The plan shall include these elements, as appropriate: (1) a detailed listing of specific tasks and procedures to implement and control these tasks; (2) a current description of each task to be performed whether or not it is already documented in existing directives; (3) identification of the organizational

unit with the authority and responsibility for executing each task; (4) the method of control to insure execution of each task as planned; (5) the schedule start and completion dates of each task; (6) identification of known technical problems to be solved; (7) an assessment of impact of these problems on specified program requirements; (8) detailed proposed solutions to the problems and a program to solve the problem; (9) procedures for recording status of actions to resolve problems; (10) method of dissemination of the system safety requirements to designers and associated personnel to expedite correction of known deficiencies; (11) designation of milestones, definition of interrelationships, and estimation of times required for system safety program activities and tasks; (12) periodic status recording of progress achieved in reducing or eliminating identified hazards and (13) delineation of the data and analyses required of and to the participating organizations.

4.1.3 Program Review

The plan shall schedule reviews to assess the safety status as part of each key program milestone. As the project develops, system safety progress shall be assessed by results of succeeding design reviews and tests, including effects of human performance.

4.2 HAZARD ANALYSES

The safety plan shall provide for the periodic performance and refinement of hazard analyses; and periodic assessment of achieved versus specified requirements for all specified missions or operational modes of the system. These studies shall include the environmental conditions of operational use, and the effect of human and equipment failure on the safety of the system. The results of hazard analyses will be employed in eliminating and controlling critical hazards and, as necessary, in the preparation of specifications, procedures, and program milestone reviews.

4.2.1 Preliminary Analyses

Preliminary analyses shall be conducted early in the Preliminary Analyses and Definition phases to provide a comprehensive, qualitative analysis of the system/subsystem/equipment in its intended operating environment for detecting and defining its potential hazards. Such information shall be used

in the development of safety criteria to be included in the performance/ design specifications. Consideration should be given to at least the following areas:

a. Isolation of energy sources.
b. Fuels and propellants: their characteristics, hazard levels and quantity/distance constraints; handling, storage, and transportation safety features; compatibility factors, etc.
c. Proposed system environmental constraints.
d. Use of explosive devices and their hazard constraints.
e. Compatibility of materials.
f. Effect of transient current, electromagnetic radiation, and ionizing radiation. Design of controls to prevent inadvertent activation of initiation circuits.
g. Use of pressure vessels and associated piping.
h. Crashworthiness for manned systems.
i. Documentation for safe operation and maintenance of the system.
j. Training and certification pertaining to safe operation and maintenance of the system.
k. Egress, rescue, survival, and salvage.
l. Life support requirements and its safety implications in manned systems.
m. Fire sources and protection.
n. Resistance to shock damage.
o. Equipment layout and lighting requirements and their safety implications in manual system.
p. Nuclear and isotope power sources or experiments.
q. System interactions.
r. Meteoroid penetration.
s. Docking consideration.
t. Long term storage.

4.2.2 Detailed Hazard Analyses

The preliminary analyses for hazard identification initiated in the Preliminary Analysis Phase shall be expanded in depth in the Definition and Design Phases. These analyses are to include the systems and subsystems equipment and their interfaces. Catastrophic hazards shall be eliminated or controlled. Results of analyses which indicate unresolved catastrophic and critical hazard categories shall be immediately reported to the procuring activity by Safety Analysis Reports (SAR). Nuclear systems will meet a negligible hazard category unless a waiver is granted.

4.2.3 Operating Hazard Analyses

Analyses shall be conducted to determine safety requirements for personnel, procedures, and equipment used in installation, maintenance, support, testing, operations, emergency escape, egress, rescue, and training. Results of these analyses shall provide the basis for: (1) design changes, where feasible, to eliminate hazards or provide safety devices, safeguards, etc; (2) inputs to the warning, caution, and emergency procedures section of test operating and maintenance procedures and instructions; (3) identification of a hazardous period time span and actions required if such hazards occur; and (4) special procedures for servicing, handling, storage and transportation.

4.3 HAZARD REDUCTION PRECEDENCE SEQUENCE

Actions for reducing hazards identified in above analyses shall be, in order of precedence, as specified in paragraphs 4.3.1 through 4.3.5 of these requirements.

4.3.1 Design for Minimum Hazard

The major effort throughout the design phases shall be to insure inherent safety through the selection of appropriate design features as fail safe, redundancy, and increased ultimate safety factor.

4.3.2 Safety Devices

Known hazards which cannot be eliminated through design selection shall be reduced to the acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.

4.3.3 Warning Devices

Where it is not possible to preclude the existence or occurrence of a known hazard, devices shall be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application shall be designed to minimize the probability of wrong signals or of improper personnel reaction to the signals.

4.3.4 Special Procedures

Where it is not possible to reduce the magnitude of an existing or potential hazard through design, or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations shall be standardized in accordance with the direction of the procuring activity.

4.3.5 Residual Hazards

Residual hazards for which safety or warning devices and special procedures cannot be developed or provided for counteracting the hazard shall be specifically identified to safety and program management. Continuation of effort to eliminate or reduce such hazards shall be accomplished throughout the program by maintaining awareness of new safety technology or devices being developed and their application to the residual hazards. Justification for the retention of residual hazards shall be documented.

4.4 SAFETY TRAINING AND CERTIFICATION

Safety information on approved methods and procedures will be included in the proficiency certification training of operational personnel in hazardous operations. A current status of certification will be maintained and oriented to missions, configurations and locations. Protective devices and emergency equipment will be identified and included. Hazards will be brought to the attention of trainees. Proficiency demonstrations of training are required for hazardous operations.

4.5 HUMAN ENGINEERING

Procedures shall be developed to assure the application of safety related human engineering principles during design, development, manufacture, test, maintenance, and operation of the system or subsystem to minimize human error.

4.6 INTERFACE WITH OTHER PROGRAM FUNCTIONS

The safety program shall be coordinated with the other program functions to avoid overlaps and conflicts between the technical disciplines, and to

establish an integrated effort. This coordination shall include: the delineation of responsibilities, management structure, joint analyses, reporting procedures, feedback of testing data and corrective actions, use of failure mode and effects analysis or other analytical techniques to identify hazards.

4.7 INDUSTRIAL SAFETY AND PUBLIC SAFETY

The system safety program will include coordination with the industrial and public safety efforts to ensure an effective and integrated total safety effort.

4.8 HAZARD DATA COLLECTION, ANALYSIS AND CORRECTIVE ACTION

Using existing data systems wherever practical, a system for hazard reporting, data storage, and feedback of corrective action shall be formulated. This will involve a closed-loop system for collecting, analyzing, and recording all reported hazards that occur in-plant or at installation sites.

4.9 SAFETY DATA

Safety data provided by the procuring activity shall be used as a design aid to prevent repetitive design deficiencies.

Data prepared in connection with analyses and studies conducted in compliance with this document shall be delivered in accordance with paragraph 6.2.

4.10 MISHAP INVESTIGATION AND REPORTING

All mishaps (including accidents/incidents) will be investigated, utilizing applicable techniques as contained in the Accident/Incident/Mission Failure Reporting and Investigation Handbook for cause(s) and system safety implications. The findings, conclusions, and recommendations will be documented and provided to the appropriate action agencies for disposition. The contractor shall be prepared to provide technical assistance to boards investigating mishaps which occur within his jurisdiction.

SYSTEM SAFETY REQUIREMENTS FOR
MANNED SPACE FLIGHT

SECTION 5

SYSTEM SAFETY IMPLEMENTATION ASSURANCE

5.1 MARGIN OF SAFETY TESTING

Provisions shall be made to assure that adequate validation tests are performed on critical devices or components to determine the degree of hazard or margin of safety of design. Induced failure tests should also be considered for demonstrating the failure mode of critical components.

5.2 SAFETY MONITORING

Observation of designated hazardous/dangerous operations will be accomplished as necessary to insure adherence to safety principles and compliance with safety requirements and checklists. Normally, the degree of monitoring necessary (spot-check, full time monitoring, etc.) will vary depending upon such factors as: the nature of the operation; the history/experience; the quality of technical data available; the personnel involved and the type of facilities available. Other factors may also be decisive and the degree of monitoring required should be periodically evaluated as the state-of-the-art progresses.

5.3 SAFETY AUDITS

The Program Safety Function will audit the Centers' compliance with established safety requirements, assuring that adequate requirements have been placed on their contractors and that each contractor has developed and is implementing a System Safety Plan applicable to his contract end items.

Center Safety Functions will audit the Centers' implementation of established safety requirements and their contractors' safety program performance. The contractors will audit their own conformance to safety requirements and the performance of their subcontractors and suppliers, as appropriate.

These audits will evaluate the degree of conformance to the established safety requirements. Requirements audited will also include safety requirements specified in design, manufacturing, test and operational specifications.

5.4 REVIEW OF CHANGES

When changes are proposed for equipment design or procedures, analyses will be performed for the proposed configuration to identify and resolve possible hazards that may be introduced into the system. The results of these analyses shall be provided to the Configuration Control Board (CCB) for consideration.

5.5 POSTFLIGHT EVALUATION

Safety personnel shall participate in postflight reviews and obtain a safety evaluation of areas in which anomalous conditions were revealed. This safety evaluation will provide guidance in planning future missions and establishing necessary corrective action to reduce hazards. Areas for consideration include:

a. Safety adequacy of procedures and protective equipment.
b. Response of warning devices and effectiveness of emergency procedures and equipment.
c. Effects of unforecast and unpredicted events.
d. Effects of human capabilities and constraints on Crew Safety.
e. Provision for pertinent inputs to data file.
f. Assuring that applicable activities receive pertinent information for appropriate corrective actions.

5.6 DATA REQUIREMENTS

The selected data requirements in support of this document will be reflected in the Contractor Data Requirements List (NASA Form 1106), attached to the request for proposal, invitation for bid, or the contract, as appropriate. All safety data developed on a program shall be filed, maintained and made available for review and use by authorized representatives of the procuring activity upon request.